International View of the State-of-the-Art of Cryptography and Security and its Use in Practice (VIII)

Friday December 4

Venue: University of Auckland

Participation:

Please contact Claire Vishik (claire.vishik@intel.com) if interested in participation and/or presenting. There is no registration or attendance fee.

Workshop Description

The goal of the workshop series is to provide a forum for an informal to exchange opinions or provide updates on issues associated with the design, implementation, and use of commercial cryptography and secure computation.

Building on the ***International View of the State-of-the-Art of Cryptography and Security and its Use in Practice*** workshops in Dagstuhl in 2011, Beijing in 2012 Athens and Bangalore in 2013 Copenhagen and Kaosiung in 2014, and Sofia in 2015, we will meet again in Auckland following Asiacrypt 2015 to bring together researchers from Europe, Asia, and the Americas hailing from industry, academia, and government.

The one day workshop in Auckland will discuss directions and developments in theoretical and applied cryptography and surrounding societal and regulatory issues.

Based on suggestions of the workshop community, we will be covering several broad topics including (but not limited to):

- Areas of research focus: lightweight cryptography, homomorphic encryption, secure computation, key management, algorithms design and evaluation
- Policy, regulatory, and cryptography usage environment, including privacy
- Innovative use cases and ideas for cryptography, e.g., in Smart Cities context
- Updates on cryptography-related research projects

We invite those interested in attending the workshop to send topics of interest to them and proposals for talks and/or discussions. On December 4th, we will follow the format we used for the last five workshops: the focus areas will be anchored by an invited talk and/or panel of short talks, and the emphasis will be on discussion and exchange of opinions. A students session may be part of the workshop.

The program will be posted here as it firms up; updates will be also distributed by email to the workshop email list.

Workshop Program

9:00-9:20am	20 min	Opening statements, introductions – organizers
9:20-10:40am	80 min	Session 1 (Potential) students projects session Discussion
10:40-11:00am	20 min	Break
11:00-12:30pm	90 min	Session 2: Novel areas of cryptography Discussion
12:30-1:30pm	60 min	Lunch
1:30-3:00pm	90 min	Session 3. Applications Discussion
3:00-3:15pm	15 min	Break
3:15-4:30pm	75 min	Session 4. Privacy and related issues
4:30pm-5pm	20 min	Post workshop: Future topics, suggested format. Adjourn